Completeness and discrimination of hazard analyses

Taylor, J.R.

Publication date:
1981

Document Version
Publisher's PDF, also known as Version of record

RISØ-M-2306

COMPLETENESS AND DISCRIMINATION OF HAZARD ANALYSES

J. R. Taylor

Abstract. "Completeness" is a necessity in any form of hazard identification or risk analysis. The analyst should know just which types of hazards he has found, and which remain uninvestigated. However, the theoretical framework for discussion of this problem has until now been missing. This report provides the theoretical framework from a parallel report (1). It investigates the completeness properties of a size risk analysis procedure in practice, during the construction and operation of a chemical plant.

INIS-descriptors HAZARDS; INDUSTRIAL PLANTS; POWER PLANTS; RISK ANALYSIS.

UDC 614.8

Presented at SCRATCH Seminar 5, Bornholm, May 1981.

September 1981
Risø National Laboratory, DK 4000 Roskilde, Denmark

ISBN 87-550-0786-4
ISSN 0418-6435

Risø Repro 1981

CONTENTS

INTRODUCTION

One of the traps facing any risk analyst is that he completes an analysis, only to have the plant undergo a major disaster which was overlooked in his analysis. Nearly as bad is for a major omission to be found as a result of actual failures, even if a disaster does not result. This is surprisingly likely to happen. It has happened for WASH 1400 (Browns Ferry fire, possibly, and Three Mile Island), and for the Canvey Island study (LNG level switches). If risk analyses are to retain their credibility, then it will be necessary to describe what the intended coverage is, and what types of hazard can be expected to have been overlooked.

When risk analysis is used as an aid in the design, the omissions in hazard identification constitute more than just a professional embarrassment. Omissions can be responsible for causing accidents, in the sense that appropriate safety equipment may be left out of the design, or especially hazardous features may be built in.

In order to be able to discuss the problem of coverage or completeness of risk analyses, a theoretical framework is required. This paper presents such a framework. Further, experimental results are presented which show the kinds of completeness problems which are likely to arise, and the degree of completeness which can be expected for several analysis methods. The results are drawn from about four full scale commercial risk analysis projects in the chemical industry, and an experimental project in which many different methods were applied to the same batch processing plant at different construction stages, starting with the initial flow sheet, and continuing through to full production.

A general framework for analysis completeness

If hazards are identified in an analysis, there are two possible fates for them. Either the hazards are tolerated, or they are eliminated. But to expect perfect identification is foolish. Some hazards will remain unidentified because the methods used for identification are imperfect. But even with perfect methods, some hazards would remain unidentified because of lack of knowledge. The knowledge may be unavailable to the engineering community as a whole.

As an example of lack of knowledge leading to oversights, the phenomenon of zinc embrittlement of hot steel was virtually unknown outside the research laboratories before the Flixborough enquiry. As another example, the phenomeon of cosmic alpha particle disturbance of computer circuits has only been recognised within the last few years.

Even if a very complete hazard analysis has been produced, its value can be undermined because safety management is inadequate. New hazards can be introduced because of management actions or oversights. In making any risk analysis it is necessary to make assumptions, including assumptions about how the plant will be managed. For example, it may be assumed that safe working procedures will be used in clearing flammable atmospheres before welding begins. If management allows such procedures to be ignored, then new hazards will be introduced which are not included in the hazard analysis.

Studies of hazard analysis completeness will therefore always be subject to uncertainty regarding lack of knowledge, and to assumptions regarding adequacy of safety management.

Degree of analysis detail

All process plant accident hazards can be classified as explosions, fires, drownings and asphyxiations, and mechanical impact and cutting accidents. This list is complete, with some

reservations for the definition of the word "accident". The list is not very detailed, however, and not very useful.

As the degree of detail in an analysis increases, the scope for omission increases. Generally, the degree of completeness decreases also. Any discussion of completeness of an analysis, then, must first include a definition of the level of analysis detail.

In the discussion of practical risk analysis trials described later, the degree of detail assumed is that of failure modes of individual components at the decomposition level where valves, pumps, filters and switches are typical. Analyses with a finer degree of detail are possible, such as individual vessel fittings, transistors, or switch springs. Similarly, it is possible to break analyses down into causes of component failure, such as corrosion, vibration, overloading, under-dimensioning etc. In the later discussion of practical experience such more detailed analyses will not be covered.

It is possible to carry out risk analyses on a less detailed level, where subsystems such as distillation columns, storage tanks, and chemical reactors are regarded as components. At even less detailed levels, a complete refinery or ammonia storage installation might be considered as a unit. Risk analyses are then based on statistical data from similar plant, perhaps with scaling factors to modify for size of plant.

Such analyses will in principle give a complete coverage of the more common risks, depending on the amount of experience available. For example, if a few hundred system years of experience is available, then risks arising once per ten years should be reasonably well covered. Such analyses will not, though, indicate how to make detailed design improvements, and can be invalidated if there are just a few non-standard design details.

Measures of completeness

A simple measure of completeness of hazard analyses would be

$$\frac{\text{Number of hazards identified}}{\text{Number of possible hazards}}$$

If this ratio has the value 1, then the analysis could be said to be absolutely complete.

Such a measure is useless in practice, because, as indicated earlier, it is impossible to know when all possible hazards have been found.

A more practical measure is historical completeness. This is defined as

$$\frac{\text{Number of hazards identified by a particular method}}{\text{Number of hazards which can be identified in the plant from a standard list of case stories}}$$

This is the measure which has been used by the author in practical studies. For this purpose the historical basis which was used is the collection of case stories in "Loss Prevention", and "Loss Prevention Bulletin". For study purposes these hazards have been extracted and drawn out as a "generic fault tree" |1|.

Some hazard identification methods treat a specific class of hazards which is logically complete. Such completeness within a method defined class of hazards can be termed internal completeness. Failure mode and effects analysis is an example of a method for which at least the starting point (individual component failure modes) is logically complete.

For methods which are in principle internally complete, two interesting questions arise. First, to what extent is the theoretical completeness achieved in practice (simple clerical errors, or mistakes, can prevent the ideal from being achieved). Second, given a complete identification of a class of

hazards, what hazards lie outside this class. This second question is very important, because its answer will indicate how particular hazard analyses should be supplemented using alternative methods.

In some cases, hazards are deliberately excluded from an analysis in order to reduce the effort involved. For example only single or double failure hazards may be included, or only failure combinations occuring more frequently than once per thousand years. Such cut-off rules are typically used to avoid drowning analyses in insignificant detail.

When such cut-off rules are used, a better measure of completeness is the proportion of historical risk analysed, defined by

$$\frac{\sum f_i c_i \text{ for all hazards identified}}{\sum f_i c_i \text{ for all hazards from a case story list which could be identified}}$$

Discrimination

When a hazard has been identified as a potential source of risk, it is often necessary to perform further calculations to confirm that the hazard can actually arise. For example, cooling pump failure may lead to a chemical reactor overheating. Whether the temperature reached will be high enough to cause a runaway reaction will depend on the rate of heat generation and on the natural convection cooling. To decide whether the hazard is actual will require a fairly lengthy calculation and possibly some experiment. Alternatively a judgement may be made about the degree of hazard.

Such judgements, made to avoid calculation work, introduce chances for hazards to be omitted which should be included in an anlysis. They also make it possible to include hazards in an analysis which cannot occur in practice.

A measure of discrimination for a hazard analysis can be defined as

$$\frac{\text{The number of hazards in the plant hazard list which can actually occur}}{\text{The total number of hazards identified in the plant hazard list}}$$

This measure can be determined by taking a hazard analysis, and checking the listed hazards very carefully. It has been observed that when good hazard analysis methods are used, the main difference between experienced and inexperienced analysts is that the experienced analysts achieve a higher degree of discrimination.

The desire for a high degree of completeness obviously conflicts with the desire for high discrimination, especially if the time available for analysis is limited, as it often is in industrial work.

Evaluation of completeness and discrimination

Evaluation of completeness can be achieved by comparing different analyses, by comparing with case story collections, and by following the plant analysed through commissioning and operation. All of these approaches have been used in the analysis experiments described here.

Practical evaluation of completeness 1

Hazard and operability analysis

Hazard and operability analysis is one of the most popular approaches to hazard identification for process plant. The version studied here is one developed from Lawley's original method, with the aim of achieving a defined degree of completeness. The plant is divided into "vessels" or "volumes", and for

each a range of variables is studied. The variables chosen should be a thermodynamically complete set, and the ones chosen here are temperature, pressure, level concentration of various substances, degree of mixing, surface tension, charge etc. For each of these the causes and consequences of variations too high and too low are studied. Additionally the variation "breach of pressure boundary" is studied. Causes and consequences are drawn up in tabular form.

Through the course of about ten analyses, a check list of causes has been built up, and included in standard analysis sheets. It has been observed that this greatly increases completeness (by about a factor of two) even when compared with analyses performed by experienced engineers.

The method is typically applied to flow sheets and piping and instrumentation diagrams. This in itself limits the hazard analysis, since height effects such as air locks, head effects, proximity effects, and mechanical details are not well treated.

Using the best available check list support, for a batch distillation plant 30 hazards were identified using the method. Subsequently the list of hazards was extended to 124 items, giving the degree of completeness of the method in this case of about 25% [2].

The use of the hazard and operability method on a batch process is perhaps an unfair test. It is really intended to treat divergences from a steady state of operation. The starting point for the procedure is itself logically complete provided that the plant is sufficiently finely divided up into volumes. The main problem which restricts the method seems to be that it does not lead the analyst to think of correct sequential functioning of plant equipment, and therefore does not indicate departures from correct functioning.

Where complex piping or control wiring is used in a plant, filling out cause and consequence columns of analysis tables can be very complicated. In such cases it is better to extend

the analysis, so that it is carried out on a line by line basis, using high and low temperature, concentration, impurities, and high, low, zero, and reverse flow as guides to search. Alternatively, fault trees can be constructed to fill out cause columns, and consequence diagrams to fill out consequence columns. This extension added two additional hazards to the 30 identified by the volume and volume method.

In any case, hazard and operability studies should be supplemented by examination of reaction potential (reaction matrices) since the method does not in itself provide much guidance for treating these.

Practical evaluation of completeness 2

Action error analysis

This method is a version of cause consequence analysis used to treat operating procedures. Operating procedures are written down action by action, and the effect on the plant of each action is noted. Then the effect of a range of possible errors for each action is considered, and the effect of the correct action for a range of abnormal states of the components affected by the action. The action errors and plant events are drawn up on diagrams for which preprinted forms have been prepared.

The range of errors treated is:

ACTION - TOO EARLY
TOO LATE
TOO MUCH
TOO LITTLE
TOO LONG
TOO SHORT
WRONG DIRECTION

ON WRONG OBJECT
WRONG ACTION

This set of errors is logically complete, but the list of WRONG ACTIONS must be limited in some way, for practical purposes. Also it is generally necessary to limit the number of failures and errors treated in any sequence to three or four. Otherwise the analysis becomes very lengthy and confusing.

In practice, for the batch plant analysis, the action-error method applied after the hazard and operability method revealed a further 82 hazards, giving a degree of completeness of about 66%, and bringing the completeness of the hazard and operability and action error methods together up to 90%. While 12 plant modifications were made on the basis of the hazard and operability analysis, a further 30 were made on the basis of the action error analysis.

Practical evaluation of completeness 3

On site checks

Many hazards can only be observed by inspecting the plant itself. For example, cables running over sharp edges cannot be seen on drawings. Nor can dirt blocking safety drains.

In the batch distillation plant study inspection check lists were used as well as item by item inspection. A further ten hazards were discovered in this way. A further three were only identified as a result of disturbances arising during commissioning.

Practical evaluation of completeness 4

Comparison with case stories

As described earlier, a few thousand case stories were studied, and their hazard mechanisms drawn up on a generic fault tree. This proved to be a very effective way of checking the earlier analyses. The comparison took only about two hours. A further two hazards were revealed. This means that a good estimate of completeness for the hazard and operability analyses, action-error analysis, and commissioning checks together was 97%. Of course different results might be found on other plants. Even if other hazards are discovered later, the percentages given here should not change very much. The 3% of hazards which were not found by the analyses might not be worrying in the case of plant approval risk assessments, but they are quite disturbing for analyses in support of plant design. On the other hand it is estimated that only about half of the hazards would have been found during normal design activities and commissioning.

The reasons for the omissions are interesting. In one case a reaction was involved causing gas generation and scumming. The nature of the reaction is still unknown, and the problem has been solved by putting less residue in waste drums so that there is room for the scum.

A second oversight was to overlook a pipe which could hold significant quantities of methanol, which could run backwards through a pump and escape. The problem could have been seen earlier if the line by line hazard and operability procedure had been used, or if coupling and decoupling tanker connections had been included as explicit actions in the operating procedure.

In a third case an unwelded joint was not seen until water pressure testing. Such problems cannot be prevented by analysis.

In the last case, freezing of product within a condenser had been foreseen as a potential problem, but had not been given much weight. In practice cooling water temperature variations

prove to be larger than had been anticipated.

Practical evaluation of completeness 5

Probability calculations

The process of transforming hazard identification lists to probability calculations has been found to increase both completeness and discrimination. Hazards are set more firmly in perspective, and in setting probabilities for one hazard cause, other possible causes are suggested.

In full scale commercial studies of this effect has been found to increase completeness by one or two percent.

Practical Evaluation of completeness 6

Fault tree analysis

Fault tree analysis applied manually at the component failure mode level has been found to suffer from several problems, in particular poor treatment of short circuit, burst pipe, erroneous valve opening or switch closing, and sequential control problems. Quite simple problems set as classroom examples have been found to be solved incorrectly, even by expert analysts. In practical use, for piping and wiring problems, a degree of completeness of about 80% has been observed, and a much lower degree of completeness for sequential control and plant operating problems.

Automatic fault tree and consequence diagram construction

These methods are currently being applied to the distillation plant example described earlier. They relate hazards directly

to disturbances described by mass and energy balance equations, and similar physical equations, and thoroughly developed failure mode lists for individual components. The methods have an internal completeness property, and treat thoroughly all disturbances arising in plant variables as a result of component failures and the action errors described earlier.

Comparison with the batch distillation plant manual analysis indicates that the hazards found by the hazard and operability analysis and the action error analysis are found, and that two of the errors found by on site checks were also found. The level of discrimination was lower, however. Studies are still in progress. Current results indicate that a degree of completeness of 94% should be achieved, and togetner with on site checks about 98%.

Theoretically, the methods should lead to oversights where the model on which the analysis is based does not correspond to the actual plant. This will occur if drawings are not "as built", and if construction details are of low standard. Additionally, with the methods used, hazards arising as a result of potential energy of height are not included. As for all flow sheet or piping and instrumentation diagram based methods, mass and energy storages and flows, and substances and reactions which are not included in the analysts model will be omitted. This does not seem to have been significant in the present study.

CONCLUSIONS

Different hazard analysis methods reveal different hazard types, and a range of methods is necessary if all hazards are to be detected. Absolute perfection cannot be expected. If the less time consuming methods are applied first, then a situation with diminishing returns will arise, where the more expensive methods reveal fewer problems, (. g. 2). At some stage the

costs of analysis will break even with the benefits arising from hazard reduction and elimination of commissioning and operating problems. The break even point will occur where the slope of the cost benefit curve is one, that is increase in cost equals increase in benefit. Monetary values can now be set on this curve, and some estimate can be made of the risk remaining after different types of hazard analysis have been performed for process plant.

ACKNOWLEDGEMENTS

The work reported here was supported by the Danish Technical Council and Risø National Laboratory. It was made possible by the help and cooperation of Grindsted Products A/S. The author would like to thank O. Hansen, S. Kjærsgaard, C. Jensen, and M. Justesen who participated in the practical studies.

REFERENCES

|1| J. R. Taylor, A Background to Risk Analysis, Risø National Laboratory, 1979. Available from the author.

|2| J. R. Taylor et al., Risk Analysis of a Batch Distillation Plant. Risø-M-2319.

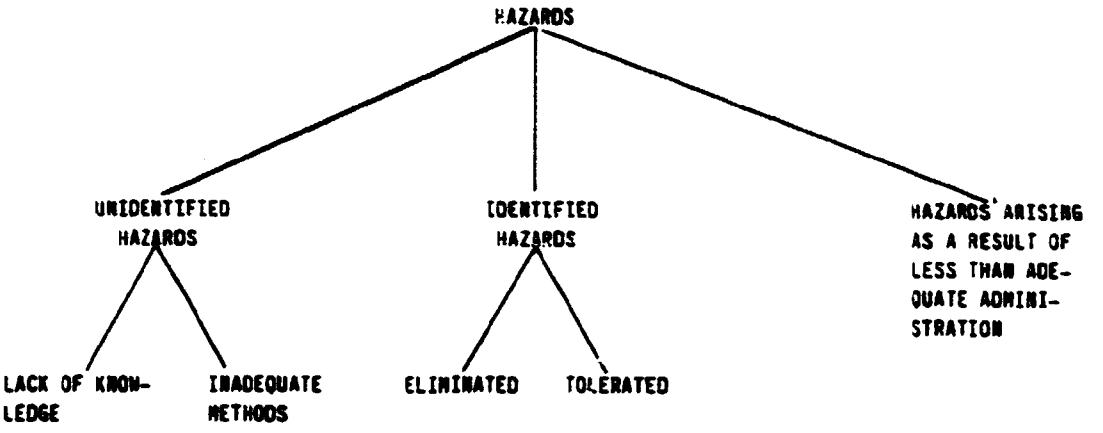

Fig. 1.: Hazard classes.

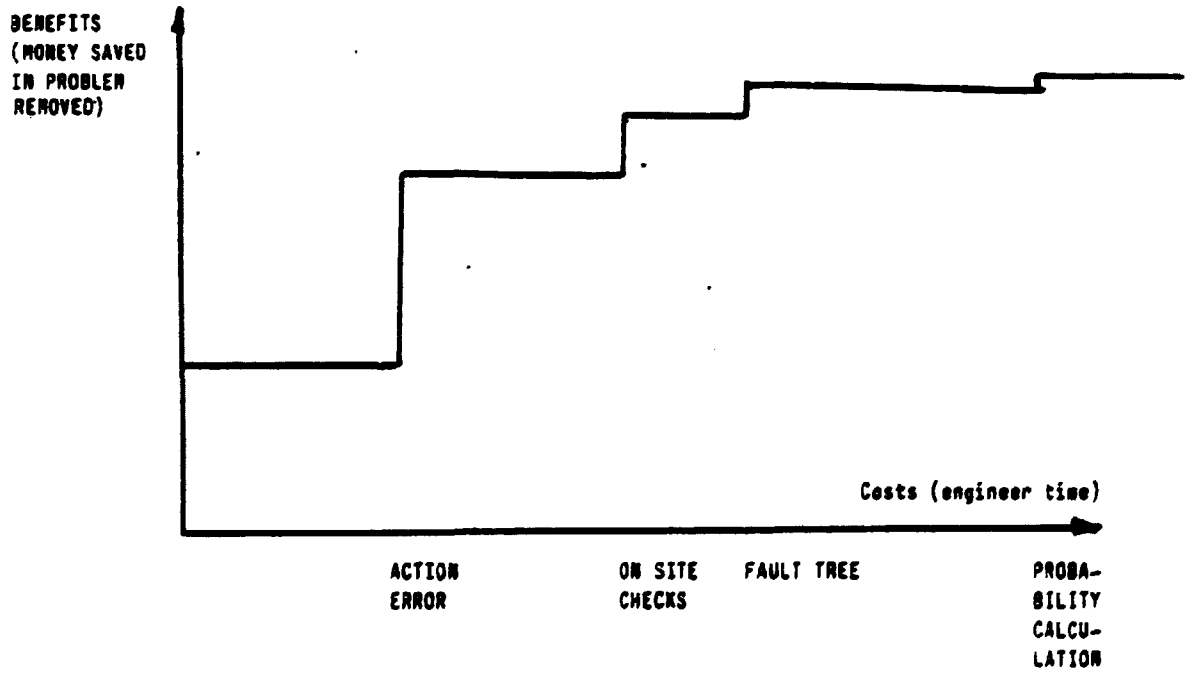

Fig. 2.: Hazard analysis break even curve.

Risø National Laboratory **Risø - M - 2306**

Risø - M - 2306

Title and author(s)

Completeness and discrimination of hazard analyses

J. R. Taylor

Date September 1981

Department or group

Electronics

Group's own registration number(s)

R-6-81

/AME

19 pages + tables + illustrations

Abstract

"Completeness" is a necessity in any form of hazard identification or risk analysis. The analyst should know just which types of hazards he has found, and which remain uninvestigated. However, the theoretical framework for discussion of this problem has until now been missing. This report provides the theoretical framework from a parallel report (1). It investigates the completeness properties of a size risk analysis procedure in practice, during the construction and operation of a chemical plant.

Copies to

Available on request from Risø Library, Risø National Laboratory (Risø Biblictek), Forsøgsanlæg Risø), DK-4000 Roskilde, Denmark
Telephone: (03) 37 12 12, ext. 2262. Telex: 43116